The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
04/04/2016

SUBJECT:
Multiple Vulnerabilities in PHP Could Allow For Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in PHP, the most severe of which could allow an attacker to potentially execute arbitrary code. PHP is a programming language originally designed for use in web-based applications with HTML content. PHP supports a wide variety of platforms and is used by numerous web-based software applications. Successfully exploiting these issues could allow remote attackers to execute arbitrary code in the context of the affected application.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild. There is known proof-of-concept code for these vulnerabilities.

SYSTEM AFFECTED:
- PHP 7 prior to 7.0.5
- PHP 5.6 prior to 5.6.20
- PHP 5.5 prior to 5.5.34

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
PHP has released updates that address multiple vulnerabilities, the most severe of which, could allow for arbitrary code execution. These vulnerabilities include:

PHP Prior to 7.0.5

- Bug 71756 (Call-by-reference widens scope to uninvolved functions when used in switch).
- Bug 71729 (Possible crash in zend_bin_strtod, zend_oct_strtod, zend_hex_strtod).

- Bug 71695 (Global variables are reserved before execution).
- Bug 71629 (Out-of-bounds access in php_url_decode in context php_stream_url_wrap_rfc2397).
- Bug 71622 (Strings used in pass-as-reference cannot be used to invoke C::$callable()).
- Bug 71596 (Segmentation fault on ZTS with date function (setlocale)).
- Bug 71535 (Integer overflow in zend_mm_alloc_heap()).
- Bug 71470 (Leaked 1 hashtable iterators).
- Bug 71575 (ISO C does not allow extra ';' outside of a function).
- Bug 71724 (yield from does not count EOLs).
- Bug 71767 (ReflectionMethod::getDocComment returns the wrong comment).
- Bug 71806 (php_strip_whitespace() fails on some numerical values).
- Bug 71624 (`php -R` (PHP_MODE_PROCESS_STDIN) is broken).
- Bug 69953 (Support MKCALENDAR request method).
- Bug 71694 (Support constant CURLM_ADDED_ALREADY).
- Bug 71635 (DatePeriod::getEndDate segfault).
- Bug 71527 (Buffer over-write in finfo_open with malformed magic file).
- Bug 71536 (Access Violation crashes php-cgi.exe).
- Bug 71906 (AddressSanitizer: negative-size-param (-1) in mbfl_strcut).
- Bug 47803, #69526 (Executing prepared statements is succesfull only for the first two statements).
- Bug 71659 (segmentation fault in pcre running twig tests).
- Bug 54648 (PDO::MSSQL forces format of datetime fields).
- Bug 71625 (Crash in php7.dll with bad phar filename).
- Bug 71317 (PharData fails to open specific file).
- Bug 71860 (Invalid memory write in phar on filename with \0 in name).
- Fixed crash when advancing (except step) inside an internal function.
- Bug 71683 (Null pointer dereference in zend_hash_str_find_bucket).
- Bug 71704 (php_snmp_error() Format String Vulnerability).
- Bug 71617 (private properties lost when unserializing ArrayObject).
- Bug 71660 (array_column behaves incorrectly after foreach by reference).
- Bug 71798 (Integer Overflow in php_raw_url_encode).

PHP Prior to 5.6.20

- Bug 69953 (Support MKCALENDAR request method).
- Bug 71596 (Segmentation fault on ZTS with date function (setlocale)).
- Bug 71694 (Support constant CURLM_ADDED_ALREADY).
- Bug 71635 (DatePeriod::getEndDate segfault).
- Bug 71527 (Buffer over-write in finfo_open with malformed magic file).
- Bug 71906 (AddressSanitizer: negative-size-param (-1) in mbfl_strcut).
- Bug 47803, #69526 (Executing prepared statements is succesfull only for the first two statements).
- Bug 71860 (Invalid memory write in phar on filename with \0 in name).
- Bug 54648 (PDO::MSSQL forces format of datetime fields).
- Bug 71625 (Crash in php7.dll with bad phar filename).
- Bug 71504 (Parsing of tar file with duplicate filenames causes memory leak).
- Bug 71704 (php_snmp_error() Format String Vulnerability).
- Bug 71798 (Integer Overflow in php_raw_url_encode).

PHP Prior to 5.5.34

- Fixed Bug 71527 (Buffer over-write in finfo_open with malformed magic file).
- Fixed Bug 71906 (AddressSanitizer: negative-size-param (-1) in mbfl_strcut).
- Fixed Bug 71860 (Invalid memory write in phar on filename with \0 in name).
- Fixed Bug 71704 (php_snmp_error() Format String Vulnerability).
- Fixed Bug 71798 (Integer Overflow in php_raw_url_encode).

RECOMMENDATIONS:

The following actions should be taken:

- Upgrade to the latest version of PHP immediately, after appropriate testing.
- Apply the principle of Least Privilege to all systems and services.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Limit user account privileges to only those required.

REFERENCES:

PHP:
http://php.net/ChangeLog-5.php#5.5.34
http://php.net/ChangeLog-5.php#5.6.20
http://php.net/ChangeLog-7.php#7.0.5